## **DOC IT Security Evaluation Checklist: IT Security Officer Responsibilities**

An IT Security Officer (ITSO) is a DOC employee responsible for implementing and monitoring an operating unit's IT security program. This checklist provides ITSOs with a self-assessment tool, and their supervisors with a performance evaluation to, to evaluate the level of compliance with ITSO duties as established by the

- DOC IT Security Program Policy and Minimum Implementation Standards (ITSPP),
- DOC Remote Access Policy and Minimum Implementation Standards (RASP), and
- DOC Policy on Password Management (PPM).

Thi	This is an assessment of (name/operating unit/office):					
	Self Assessment	Assessment Date:				
	Third Party Evaluation	Assessor (name/title/org.):				

Status Codes: 1 = Not Started 2 = In Process 3 = In Place

## Performance Levels:

- 1 ITSO has comprehensive IT security policies in place
- 2 ITSO has comprehensive IT security policies as well as detailed procedures in place
- 3 ITSO has comprehensive IT security policies and detailed procedures in place that are fully implemented for the operating unit's IT security program
- 4 ITSO has fully implemented and tested comprehensive IT security policies and detailed procedures in place
- 5 ITSO has fully implemented and tested comprehensive IT security policies and detailed procedures in place as part of a fully integrated IT security program

IT Security Officer (ITSO) Responsibilities		DOC Policy References	Status	Performance Level
1	Develop and maintain operating unit IT security policy, procedures, standards,	ITSPP 2.1.8		
	and guidance consistent with Departmental and federal requirements.			
2	Ensure that all systems have IT security documentation in place, including:	ITSPP 2.1.8		
	(a) Qualitative risk assessments;	ITSPP 2.1.8, 3.1.2		
	(b) Current and effective IT security plans that conform to NIST SP 800-18;	ITSPP 2.1.8, 3.5.2		
	(c) Annual system self-assessments that conform to NIST SP 800-26 guidance;	ITSPP 3.2.1.2		
	(d) Current and tested contingency plans; and	ITSPP 3.9.2		
	(e) Current certification and accreditation packages.	ITSPP 3.4.1.4		
3	Conduct self-assessments of the operating unit's IT Security Program annually,	ITSPP 2.1.8,		
	including monitoring of system user compliance with these policies, as part of	RASP, PPM, and		
	their periodic IT security self-assessment program or automated system	3(a) - (c)		
	evaluations.			
	(a) Prepare program-level self-assessments annually using NIST SP 800-26 guidance;	ITSPP 3.2.1.2		
	(b) Prepare program-level corrective action plans/plans of action and milestones (POAMs) for weaknesses found; and	ITSPP 3.2.1.5		
	(c) Track program- and system-level POAMs to completion, and provide	ITSPP 3.2.1.6,		
	monthly status updates to the Department IT Security Manager.	3.2.1.7		
4	Maintain the IT system inventory tracking and provide updated inventories to	ITSPP 2.1.8,		
	the DOC IT Security Program Manager semi-annually (March and September).	3.2.4.1		
5	Establish a process to ensure that all users (including the ITSO) receive periodic	ITSPP 2.0.1,		
	IT security awareness material and copies of rules of behavior, and are trained to	RASP, PPM, and		
	fulfill their IT security responsibilities. Ensure that IT security awareness and	5(a)-(b)		
	training programs address DOC policies.			

v1 02/28/2003

all Pistablish procedures for an IT security awareness and training program for all operating unit personnel, including specialized training as necessary for system administrators, ITSOs, procurement staff, etc.  (b) Participate in training to maintain ITSO knowledge, skills, and abilities.  3.14.11  6 Act as the operating unit's central point of contact for all incidents, develop ITSPP 2.1.8, incident handling procedures, and report all incidents to the DOC CIRT.  3.14.6  7 Provide risk management information to systems administrators and others.  8 Participate as a voting member of the DOC IT Security Coordinating Committee (ITSCC), participate in special committees under the ITSCC, and provide other support for the ITSCC as appropriate.  9 Coordinate with the DOC IT Security Program Manager and CIPM, as well as OSY and OIG as appropriate on IT security malters.  10 Establish a process to ensure access privileges are revoked in a timely manner when the requirement for access ceases (e.g., transfer, resignation, retirement, change of job description, etc.)  11 Establish a process to periodically review, on a sample basis, the licensing of software within their organization. And, report any infringements to the operating unit CIO's office.  12 Ensure that personnel security controls are addressed in operating unit IT security program policy and system security plans, including:  (b) Rules of behavior/acceptable use policies;  (c) Segregation of duties; and  (d) Personnel termination and transfer.  11 SPP 3.6.1  RASP  12 Ensure that all operating unit employees understand software copyright rules of behavior guidance.  14 Establish a process to identify, track, and report on security patch management.  15 Establish a process to identify, track, and report on security patch management.  16 Establish a process to identify, track, and report on security patch management.  17 ESPP 3.16.1  18 Ensure that tramsfer systems as commented the need for possible forensic examination of evidence for potential prosession of a	IT Security Officer (ITSO) Responsibilities		DOC Policy References	Status	Performance Level
all operating unit personnel, including specialized training as necessary for system administrators, ITSOs, procurement staff, etc.  (b) Participate in training to maintain ITSO knowledge, skills, and abilities.  6 Act as the operating unit's central point of contact for all incidents, develop incident handling procedures, and report all incidents to the DOC CIRT.  7 Provide risk management information to systems administrators and others.  8 Participate as a voting member of the DOC IT Security Coordinating Committee (ITSCC), participate in special committees under the ITSCC, and provide other support for the ITSCC as appropriate.  9 Coordinate with the DOC IT Security Program Manager and CIPM, as well as OSY and OIG as appropriate on IT security matters.  10 Establish a process to ensure access privileges are revoked in a timely manner when the requirement for access ceases (e.g., transfer, resignation, retirement, change of job description, etc.)  11 Establish a process to periodically review, on a sample basis, the licensing of software within their organization. And, report any infringements to the operating unit CIO's office.  12 Ensure that personnel security controls are addressed in operating unit IT security program policy and system security plans, including:  (a) User administration;  (b) Rules of behavior/acceptable use policies;  (c) Segregation of duties; and (d) Personnel termination and transfer.  13 Ensure that all operating unit employees understand software copyright rules of behavior guidance.  14 Establish a process to identify, track, and report on security patch management.  15 Establish a Process to identify, track, and report on security patch management.  16 Establish a process to identify, track, and report on security patch management.  17 ESPP 3.10-6.1  18 Establish a process to identify, track, and report on security patch management.  18 Establish a process to identify, track, and report on security patch management.  18 Establish a process to identify, track, and report on secur		(a) Establish procedures for an IT security awareness and training program for	ITSPP 3.13.5,		
system administrators, ITSOs, procurement staff, etc.  (b) Participate in training to maintain ITSO knowledge, skills, and abilities.  7 Provide risk management information to systems administrators and others.  8 Participate as a voting member of the DOC IT Security Coordinating Committee (ITSPC), participate in special committees under the ITSCC, and provide other support for the ITSCC as appropriate.  9 Coordinate with the DOC IT Security Program Manager and CIPM, as well as OSY and OIG as appropriate of IT security Program Manager and CIPM, as well as OSY and OIG as appropriate on IT security matters.  9 Eastablish a process to ensure access privileges are revoked in a timely manner when the requirement for access ceases (e.g., transfer, resignation, retirement, change of job description, etc.)  10 Establish a process to periodically review, on a sample basis, the licensing of software within their organization. And, report any infringements to the operating unit CIO's office.  12 Ensure that personnel security controls are addressed in operating unit IT security program policy and system security plans, including:  (a) User administrators;  (b) Rules of behavior/acceptable use policies;  (c) Segregation of duties; and  (d) Personnel termination and transfer.  13 Ensure that all operating unit employees understand software copyright rules of behavior guidance.  14 Establish a process to identify, track, and report on security patch management.  15 Establish a chain of Custody that documents (in writing) the name, title, office, and phone number of each individual having sequential possession of a system's hard drive, when it is removed due to compromise and the need for possible forensic examination of evidence for potential prosecution.  16 Establish an optimal, cost-effective, configuration for network boundary devices that includes procedures and a schedule for periodic testing of incoming filtering and 3.16.3.5 protection.  17 Ensure that cryptography is used for transmission of classified national secu			RASP, PPM		
(b) Participate in training to maintain ITSO knowledge, skills, and abilities.  TISPP 3.13.9, 3.14.11  Act as the operating unit's central point of contact for all incidents, develop incident handling procedures, and report all incidents to the DOC CIRT. 3.14.6  Provide risk management information to systems administrators and others.  Participate as a voting member of the DOC IT Security Coordinating Committee (ITSPP 2.1.8, 3.1.1)  Participate as a voting member of the DOC IT Security Coordinating Committee under the ITSCC, and provide other support for the ITSCC as appropriate.  9 Coordinate with the DOC IT Security Program Manager and CIPM, as well as OSY and OIG as appropriate on IT security matters.  10 Establish a process to ensure access privileges are revoked in a timely manner when the requirement for access ceases (e.g., transfer, resignation, retirement, change of job description, etc.)  11 Establish a process to periodically review, on a sample basis, the licensing of software within their organization. And, report any infringements to the operating unit CIO's office.  12 Ensure that personnel security controls are addressed in operating unit IT security program policy and system security plans, including:  (a) User administration;  (b) Rules of behavior/acceptable use policies;  (c) Segregation of duties; and  (d) Personnel termination and transfer.  13 Ensure that all operating unit employees understand software copyright rules of behavior guidance.  14 Establish a process to identify, track, and report on security patch management.  15 Establish a process to identify, track, and report on security patch management.  16 Establish a optimal, cost-effective, configuration for network boundary devices that includes procedures and a schedule for periodic testing of incoming filtering protection.  16 Establish a optimal, cost-effective, configuration for network boundary devices that includes procedures and a schedule for periodic testing of incoming filtering and 3.16.3.5 protection.  17 Ensure that c			,		
Act as the operating unit's central point of contact for all incidents, develop ITSPP 2.1.8, incident handling procedures, and report all incidents to the DOC CIRT. 3.14.6  7 Provide risk management information to systems administrators and others. ITSPP 2.1.8, 3.1.1  8 Participate as a voting member of the DOC IT Security Coordinating Committee (ITSCC), participate in special committees under the ITSCC, and provide other support for the ITSCC as appropriate.  9 Coordinate with the DOC IT Security Program Manager and CIPM, as well as OSY and OIG as appropriate on IT security matters.  10 Establish a process to ensure access privileges are revoked in a timely manner when the requirement for access ceases (e.g., transfer, resignation, retirement, change of job description, etc.)  11 Establish a process to periodically review, on a sample basis, the licensing of software within their organization. And, report any infringements to the operating unit CIO's office.  12 Ensure that personnel security controls are addressed in operating unit IT security program policy and system security plans, including:  (a) User administration;  (b) Rules of behavior/acceptable use policies;  (c) Segregation of duties; and (d) Personnel termination and transfer.  13 Ensure that all operating unit employees understand software copyright rules of behavior guidance.  14 Establish a process to identify, track, and report on security patch management.  15 Establish a process to identify, track, and report on security patch management.  15 Establish a process to identify, track, and report on retwork boundary devices and phone number of each individual having sequential possession of a system's hard drive, when it is removed due to compromise and the need for possible forensic examination of evidence for potential prosecution.  15 Establish an optimal, cost-effective, configuration for network boundary devices that includes procedures and a schedule for periodic testing of incoming filtering protection.  16 Establish an optimal, cost-effe			ITSPP 3.13.9,		
6 Act as the operating unit's central point of contact for all incidents, develop incident handling procedures, and report all incidents to the DOC CIRT.  7 Provide risk management information to systems administrators and others.  8 Participate as a voting member of the DOC IT Security Coordinating Committee (ITSPP 2.1.8, 3.1.1)  8 Participate as a voting member of the DOC IT Security Coordinating Committee (ITSPP 2.1.8, 2.2.1)  (ITSCC), participate in special committees under the ITSCC, and provide other support for the ITSCC as appropriate.  9 Coordinate with the DOC IT Security Program Manager and CIPM, as well as OSY and OIG as appropriate on IT security matters.  10 Establish a process to ensure access privileges are revoked in a timely manner when the requirement for access ceases (e.g., transfer, resignation, retirement, change of job description, etc.)  11 Establish a process to periodically review, on a sample basis, the licensing of software within their organization. And, report any infringements to the operating unit CIO's office.  12 Ensure that personnel security controls are addressed in operating unit IT (ITSPP 3.6.1) and security program policy and system security plans, including:  (a) User administration;  (b) Rules of behavior/acceptable use policies;  (c) Segregation of duties; and ITSPP 3.6.3  (d) Personnel termination and transfer.  13 Ensure that all operating unit employees understand software copyright rules of behavior guidance.  14 Establish a process to identify, track, and report on security patch management.  15 Establish a Chain of Custody that documents (in writing) the name, title, office, and phone number of each individual having sequential possession of a system's hard drive, when it is removed due to compromise and the need for possible forensic examination of evidence for potential prosecution.  16 Establish a optimal, cost-effective, configuration for network boundary devices that includes procedures and a schedule for periodic testing of incoming filtering and 3.16.3.5			1		
incident handling procedures, and report all incidents to the DOC CIRT.  7 Provide risk management information to systems administrators and others.  8 Participate as a voting member of the DOC IT Security Coordinating Committee (ITSCC), participate in special committees under the ITSCC, and provide other support for the ITSCC as appropriate.  9 Coordinate with the DOC IT Security Program Manager and CIPM, as well as OSY and OIG as appropriate on IT security matters.  10 Establish a process to ensure access privileges are revoked in a timely manner when the requirement for access ceases (e.g., transfer, resignation, retirement, change of job description, etc.)  11 Establish a process to periodically review, on a sample basis, the licensing of software within their organization. And, report any infringements to the operating unit CIO's office.  12 Ensure that personnel security controls are addressed in operating unit IT security program policy and system security plans, including:  (a) User administration;  (b) Rules of behavior/acceptable use policies;  (c) Segregation of duties; and (d) Personnel termination and transfer.  (c) Segregation of duties; and (d) Personnel termination and transfer.  13 Ensure that all operating unit employees understand software copyright rules of behavior guidance.  14 Establish a Chain of Custody that documents (in writing) the name, title, office, and phone number of each individual having sequential possession of a system's hard drive, when it is removed due to compromise and the need for possible forensic examination of evidence for potential prosecution.  15 Establish an optimal, cost-effective, configuration for network boundary devices that includes procedures and a schedule for periodic testing of incoming filtering protection.  16 Establish an optimal, cost-effective, configuration for network boundary devices that includes procedures and a schedule for periodic testing of incoming filtering information, in accordance with the DOC Security Manual, Chapter 22  18 Ensure th	6	Act as the operating unit's central point of contact for all incidents, develop			
7 Provide risk management information to systems administrators and others.   ITSPP 2.1.8, 3.1.1     8 Participate as a voting member of the DOC IT Security Coordinating Committee (ITSCC), participate in special committees under the ITSCC, and provide other support for the ITSCC as appropriate.     9 Coordinate with the DOC IT Security Program Manager and CIPM, as well as properties on IT security program Manager and CIPM, as well as properties on IT security matters.     10 Establish a process to ensure access privileges are revoked in a timely manner when the requirement for access ceases (e.g., transfer, resignation, retirement, change of job description, etc.)     11 Establish a process to periodically review, on a sample basis, the licensing of software within their organization. And, report any infringements to the operating unit CIO's office.     12 Ensure that personnel security controls are addressed in operating unit IT security program policy and system security plans, including:   ITSPP 3.6.1, RASP  (c) Segregation of duties; and   ITSPP 3.6.2, RASP  (c) Segregation of duties; and   ITSPP 3.6.3   (d) Personnel termination and transfer.   ITSPP 3.6.4, RASP    (e) Segregation of duties; and   ITSPP 3.6.4, RASP    (f) Personnel termination and transfer.   ITSPP 3.6.4, RASP    (f) Personnel termination of duties; and phone number of each individual having sequential possession of a system's hard drive, when it is removed due to compromise and the need for possible forensic examination of evidence for potential prosecution.   ITSPP 3.16.3.2   and 3.16.3.5   and 3.16.3.5   and 3.16.3.5   and 3.16.3.5   and 3.16.3.5   and 3.16.3.5			· · · · · · · · · · · · · · · · · · ·		
8 Participate as a voting member of the DOČ IT Security Coordinating Committee (ITSCC), participate in special committees under the ITSCC, and provide other support for the ITSCC as appropriate.  9 Coordinate with the DOC IT Security Program Manager and CIPM, as well as COORDINATED AND COSY and OIG as appropriate on IT security matters.  10 Establish a process to ensure access privileges are revoked in a timely manner when the requirement for access ceases (e.g., transfer, resignation, retirement, change of job description, etc.)  11 Establish a process to periodically review, on a sample basis, the licensing of software within their organization. And, report any infringements to the operating unit CIO's office.  12 Ensure that personnel security controls are addressed in operating unit IT security program policy and system security plans, including:  13 Ensure that all operating unit employees understand software copyright rules of behavior guidance.  14 Establish a process to identify, track, and report on security patch management.  15 Establish a Chain of Custody that documents (in writing) the name, title, office, and phone number of each individual having sequential possession of a system's hard drive, when it is removed due to compromise and the need for possible forensic examination of evidence for potential prosecution.  16 Establish an optimal, cost-effective, configuration for network boundary devices that includes procedures and a schedule for periodic testing of incoming filtering protection.  17 Ensure that remote systems are monitored for compliance with DOC policies (as Ensure that remote systems are monitored for compliance with DOC policies (as Ecchically possible)  18 Ensure that remote systems are monitored for compliance with DOC policies (as Ecchically possible)					
(c) Segregation of duties; and (d) Personnel termination and transfer.  13 Ensure that all operating unit employees understand software copyright rules of behavior guidance.  14 Establish a process to identify, track, and report on security patch management.  15 Establish a process to identify, track, and report on security patch management.  16 Establish a chain of Custody that documents (in writing) the name, title, office, and phone number of each individual having sequential possession of a system's hard drive, when it is removed due to compromise and the need for possible forensic examination of emote user access privileges when users violate DOC policies (as technically possible)  18 Ensure that remote systems are monitored for compliance with DOC policies (as technically possible)  19 Notify managers, supervisors, or COTRs to pursue appropriate disciplinary access a same provised on Time Poor (C) Process of the province of policies (as policies, and provided policies)  19 Notify managers, supervisors, or COTRs to pursue appropriate disciplinary access a construction of process to dentify to provide policies (as purposed to provide policies)  10 Coordinate with the DOC TI Security program Manager and CIPM, as well as provided the provided the provided to the provided to the provided to the provided to the provided pr					
support for the ITSCC as appropriate.  9 Coordinate with the DOC IT Security Program Manager and CIPM, as well as OSY and OIG as appropriate on IT security matters.  10 Establish a process to ensure access privileges are revoked in a timely manner when the requirement for access ceases (e.g., transfer, resignation, retirement, change of job description, etc.)  11 Establish a process to periodically review, on a sample basis, the licensing of software within their organization. And, report any infringements to the operating unit CIO's office.  12 Ensure that personnel security controls are addressed in operating unit IT security program policy and system security plans, including:  (a) User administration;  (b) Rules of behavior/acceptable use policies;  (c) Segregation of duties; and  (d) Personnel termination and transfer.  13 Ensure that all operating unit employees understand software copyright rules of behavior guidance.  14 Establish a process to identify, track, and report on security patch management.  15 Establish a process to identify, track, and report on security patch management.  16 Establish a chain of Custody that documents (in writing) the name, title, office, and phone number of each individual having sequential possession of a system's hard drive, when it is removed due to compromise and the need for possible forensic examination of evidence for potential prosecution.  17 Ensure that cryptography is used for transmission of classified national security information, in accordance with the DOC Security Manual, Chapter 22  18 Ensure that termote systems are monitored for compliance with DOC policies (as technically possible)  19 Notify managers, supervisors, or COTRs to pursue appropriate disciplinary action and termination of remote user access privileges when users violate DOC policies.					
9 Coordinate with the DOC IT Security Program Manager and CIPM, as well as OSY and OIG as appropriate on IT security matters.  10 Establish a process to ensure access privileges are revoked in a timely manner when the requirement for access ceases (e.g., transfer, resignation, retirement, change of job description, etc.)  11 Establish a process to periodically review, on a sample basis, the licensing of software within their organization. And, report any infringements to the operating unit CIO's office.  12 Ensure that personnel security controls are addressed in operating unit IT security program policy and system security plans, including:  (a) User administration;  (b) RASP  11 TSPP 3.6.1 and security program policy and system security plans, including:  (c) Segregation of duties; and  (d) Personnel termination and transfer.  12 Ensure that all operating unit employees understand software copyright rules of behavior guidance.  13 Ensure that all operating unit employees understand software copyright rules of behavior guidance.  14 Establish a process to identify, track, and report on security patch management.  15 Establish a Chain of Custody that documents (in writing) the name, title, office, and phone number of each individual having sequential possession of a system's hard drive, when it is removed due to compromise and the need for possible forensic examination of evidence for potential prosecution.  16 Establish an optimal, cost-effective, configuration for network boundary devices that includes procedures and a schedule for periodic testing of incoming filtering protection.  17 Ensure that eryptography is used for transmission of classified national security information, in accordance with the DOC Security Manual, Chapter 22  18 Ensure that remote systems are monitored for compliance with DOC policies (as technically possible)  19 Notify managers, supervisors, or COTRs to pursue appropriate disciplinary action and termination of remote user access privileges when users violate DOC policies.					
OSY and OIG as appropriate on IT security matters.  10 Establish a process to ensure access privileges are revoked in a timely manner when the requirement for access ceases (e.g., transfer, resignation, retirement, change of job description, etc.)  11 Establish a process to periodically review, on a sample basis, the licensing of software within their organization. And, report any infringements to the operating unit CIO's office.  12 Ensure that personnel security controls are addressed in operating unit IT security program policy and system security plans, including:  (a) User administration;  (b) Rules of behavior/acceptable use policies;  (c) Segregation of duties; and (d) Personnel termination and transfer.  13 Ensure that all operating unit employees understand software copyright rules of behavior guidance.  14 Establish a process to identify, track, and report on security patch management.  15 Establish a Chain of Custody that documents (in writing) the name, title, office, and phone number of each individual having sequential possession of a system's hard drive, when it is removed due to compromise and the need for possible forensic examination of evidence for potential prosecution.  16 Establish an optimal, cost-effective, configuration for network boundary devices that includes procedures and a schedule for periodic testing of incoming filtering protection.  17 Ensure that cryptography is used for transmission of classified national security information, in accordance with the DOC Security Manual, Chapter 22  18 Ensure that remote systems are monitored for compliance with DOC policies (as technically possible)  19 Notify managers, supervisors, or COTRs to pursue appropriate disciplinary action and termination of remote user access privileges when users violate DOC policies.			ITSPP 2 1 8 4 0		
Establish a process to ensure access privileges are revoked in a timely manner when the requirement for access ceases (e.g., transfer, resignation, retirement, change of job description, etc.)  11 Establish a process to periodically review, on a sample basis, the licensing of software within their organization. And, report any infringements to the operating unit CIO's office.  12 Ensure that personnel security controls are addressed in operating unit IT security program policy and system security plans, including:  (a) User administration;  (b) Rules of behavior/acceptable use policies;  (c) Segregation of duties; and (d) Personnel termination and transfer.  13 Ensure that all operating unit employees understand software copyright rules of behavior guidance.  14 Establish a process to identify, track, and report on security patch management.  15 Establish a Chain of Custody that documents (in writing) the name, title, office, and phone number of each individual having sequential possession of a system's hard drive, when it is removed due to compromise and the need for possible forensic examination of evidence for potential prosecution.  16 Establish an optimal, cost-effective, configuration for network boundary devices that includes procedures and a schedule for periodic testing of incoming filtering protection.  17 Ensure that eryptography is used for transmission of classified national security information, in accordance with the DOC Security Manual, Chapter 22  18 Ensure that remote systems are monitored for compliance with DOC policies (as technically possible)  19 Notify managers, supervisors, or COTRs to pursue appropriate disciplinary action and termination of remote user access privileges when users violate DOC policies.					
when the requirement for access ceases (e.g., transfer, resignation, retirement, change of job description, etc.)  11 Establish a process to periodically review, on a sample basis, the licensing of software within their organization. And, report any infringements to the operating unit ClO's office.  12 Ensure that personnel security controls are addressed in operating unit IT security program policy and system security plans, including:  (a) User administration;  (b) Rules of behavior/acceptable use policies;  (c) Segregation of duties; and  (d) Personnel termination and transfer.  13 Ensure that all operating unit employees understand software copyright rules of behavior guidance.  14 Establish a process to identify, track, and report on security patch management.  15 Establish a Chain of Custody that documents (in writing) the name, title, office, and phone number of each individual having sequential possession of a system's hard drive, when it is removed due to compromise and the need for possible forensic examination of evidence for potential prosecution.  16 Establish an optimal, cost-effective, configuration for network boundary devices that includes procedures and a schedule for periodic testing of incoming filtering protection.  17 Ensure that cryptography is used for transmission of classified national security information, in accordance with the DOC Security Manual, Chapter 22  18 Ensure that remote systems are monitored for compliance with DOC policies (as technically possible)  RASP  19 Notify managers, supervisors, or COTRs to pursue appropriate disciplinary action and termination of remote user access privileges when users violate DOC policies.					
change of job description, etc.)  11 Establish a process to periodically review, on a sample basis, the licensing of software within their organization. And, report any infringements to the operating unit CIO's office.  12 Ensure that personnel security controls are addressed in operating unit IT security program policy and system security plans, including:  (a) User administration;  (b) Rules of behavior/acceptable use policies;  (c) Segregation of duties; and (d) Personnel termination and transfer.  13 Ensure that all operating unit employees understand software copyright rules of behavior guidance.  14 Establish a process to identify, track, and report on security patch management.  15 Establish a Chain of Custody that documents (in writing) the name, title, office, and phone number of each individual having sequential possession of a system's hard drive, when it is removed due to compromise and the need for possible forensic examination of evidence for potential prosecution.  16 Establish an optimal, cost-effective, configuration for network boundary devices that includes procedures and a schedule for periodic testing of incoming filtering protection.  17 Ensure that cryptography is used for transmission of classified national security information, in accordance with the DOC Security Manual, Chapter 22  18 Ensure that remote systems are monitored for compliance with DOC policies (as technically possible)  Potity managers, supervisors, or COTRs to pursue appropriate disciplinary action and termination of remote user access privileges when users violate DOC policies.					
Establish a process to periodically review, on a sample basis, the licensing of software within their organization. And, report any infringements to the operating unit CIO's office.    12   Ensure that personnel security controls are addressed in operating unit IT security program policy and system security plans, including:   (a) User administration;   ITSPP 3.6.1, RASP			10101,11111		
software within their organization. And, report any infringements to the operating unit CIO's office.  12 Ensure that personnel security controls are addressed in operating unit IT ITSPP 3.6.0.1 and security program policy and system security plans, including:  (a) User administration;  (b) Rules of behavior/acceptable use policies;  (c) Segregation of duties; and  (d) Personnel termination and transfer.  ITSPP 3.6.2,  RASP  (d) Personnel termination and transfer.  ITSPP 3.6.4,  RASP  13 Ensure that all operating unit employees understand software copyright rules of behavior guidance.  14 Establish a process to identify, track, and report on security patch management.  15 Establish a Chain of Custody that documents (in writing) the name, title, office, and phone number of each individual having sequential possession of a system's hard drive, when it is removed due to compromise and the need for possible forensic examination of evidence for potential prosecution.  16 Establish an optimal, cost-effective, configuration for network boundary devices that includes procedures and a schedule for periodic testing of incoming filtering protection.  17 Ensure that cryptography is used for transmission of classified national security information, in accordance with the DOC Security Manual, Chapter 22  18 Ensure that remote systems are monitored for compliance with DOC policies (as technically possible)  RASP  19 Notify managers, supervisors, or COTRs to pursue appropriate disciplinary action and termination of remote user access privileges when users violate DOC policies.			ITSPP 3 2 1 3		
operating unit CIO's office.  12 Ensure that personnel security controls are addressed in operating unit IT security program policy and system security plans, including:  (a) User administration;  (b) Rules of behavior/acceptable use policies;  (c) Segregation of duties; and (d) Personnel termination and transfer.  13 Ensure that all operating unit employees understand software copyright rules of behavior guidance.  14 Establish a process to identify, track, and report on security patch management.  15 Establish a Chain of Custody that documents (in writing) the name, title, office, and phone number of each individual having sequential possession of a system's hard drive, when it is removed due to compromise and the need for possible forensic examination of evidence for potential prosecution.  16 Establish an optimal, cost-effective, configuration for network boundary devices that includes procedures and a schedule for periodic testing of incoming filtering protection.  17 Ensure that cryptography is used for transmission of classified national security information, in accordance with the DOC Security Manual, Chapter 22  18 Ensure that remote systems are monitored for compliance with DOC policies (as technically possible)  19 Notify managers, supervisors, or COTRs to pursue appropriate disciplinary action and termination of remote user access privileges when users violate DOC policies.			11011 5.2.1.5		
12 Ensure that personnel security controls are addressed in operating unit IT security program policy and system security plans, including:   (a) User administration;   ITSPP 3.6.1, RASP					
security program policy and system security plans, including:  (a) User administration;  (b) Rules of behavior/acceptable use policies;  (c) Segregation of duties; and  (d) Personnel termination and transfer.  1TSPP 3.6.3  (d) Personnel termination and transfer.  1TSPP 3.6.4,  RASP  13 Ensure that all operating unit employees understand software copyright rules of behavior guidance.  14 Establish a process to identify, track, and report on security patch management.  15 Establish a Chain of Custody that documents (in writing) the name, title, office, and phone number of each individual having sequential possession of a system's hard drive, when it is removed due to compromise and the need for possible forensic examination of evidence for potential prosecution.  16 Establish an optimal, cost-effective, configuration for network boundary devices that includes procedures and a schedule for periodic testing of incoming filtering protection.  17 Ensure that cryptography is used for transmission of classified national security information, in accordance with the DOC Security Manual, Chapter 22  18 Ensure that remote systems are monitored for compliance with DOC policies (as technically possible)  19 Notify managers, supervisors, or COTRs to pursue appropriate disciplinary action and termination of remote user access privileges when users violate DOC policies.			ITSPP 3 6 0 1 and		
(a) User administration; (b) Rules of behavior/acceptable use policies; (c) Segregation of duties; and (d) Personnel termination and transfer.  ITSPP 3.6.3 (d) Personnel termination and transfer.  ITSPP 3.6.4, RASP  13 Ensure that all operating unit employees understand software copyright rules of behavior guidance.  14 Establish a process to identify, track, and report on security patch management.  15 Establish a Chain of Custody that documents (in writing) the name, title, office, and phone number of each individual having sequential possession of a system's hard drive, when it is removed due to compromise and the need for possible forensic examination of evidence for potential prosecution.  16 Establish an optimal, cost-effective, configuration for network boundary devices that includes procedures and a schedule for periodic testing of incoming filtering protection.  17 Ensure that cryptography is used for transmission of classified national security information, in accordance with the DOC Security Manual, Chapter 22  18 Ensure that remote systems are monitored for compliance with DOC policies (as technically possible)  19 Notify managers, supervisors, or COTRs to pursue appropriate disciplinary action and termination of remote user access privileges when users violate DOC policies.					
(b) Rules of behavior/acceptable use policies;  (c) Segregation of duties; and  (d) Personnel termination and transfer.  ITSPP 3.6.3  (d) Personnel termination and transfer.  ITSPP 3.6.4,  RASP  13 Ensure that all operating unit employees understand software copyright rules of behavior guidance.  14 Establish a process to identify, track, and report on security patch management.  15 Establish a Chain of Custody that documents (in writing) the name, title, office, and phone number of each individual having sequential possession of a system's hard drive, when it is removed due to compromise and the need for possible forensic examination of evidence for potential prosecution.  16 Establish an optimal, cost-effective, configuration for network boundary devices that includes procedures and a schedule for periodic testing of incoming filtering protection.  17 Ensure that cryptography is used for transmission of classified national security information, in accordance with the DOC Security Manual, Chapter 22  18 Ensure that remote systems are monitored for compliance with DOC policies (as technically possible)  19 Notify managers, supervisors, or COTRs to pursue appropriate disciplinary action and termination of remote user access privileges when users violate DOC policies.					
(b) Rules of behavior/acceptable use policies; (c) Segregation of duties; and (d) Personnel termination and transfer.  ITSPP 3.6.3 (d) Personnel termination and transfer.  ITSPP 3.6.4, RASP  13 Ensure that all operating unit employees understand software copyright rules of behavior guidance.  14 Establish a process to identify, track, and report on security patch management.  15 Establish a Chain of Custody that documents (in writing) the name, title, office, and phone number of each individual having sequential possession of a system's hard drive, when it is removed due to compromise and the need for possible forensic examination of evidence for potential prosecution.  16 Establish an optimal, cost-effective, configuration for network boundary devices that includes procedures and a schedule for periodic testing of incoming filtering protection.  17 Ensure that cryptography is used for transmission of classified national security information, in accordance with the DOC Security Manual, Chapter 22  18 Ensure that remote systems are monitored for compliance with DOC policies (as technically possible)  19 Notify managers, supervisors, or COTRs to pursue appropriate disciplinary action and termination of remote user access privileges when users violate DOC policies.		(a) OSCI administration,	· · · · · · · · · · · · · · · · · · ·		
(c) Segregation of duties; and ITSPP 3.6.3  (d) Personnel termination and transfer. ITSPP 3.6.4, RASP  13 Ensure that all operating unit employees understand software copyright rules of behavior guidance.  14 Establish a process to identify, track, and report on security patch management. ITSPP 3.10.4.1 behavior guidance.  15 Establish a Chain of Custody that documents (in writing) the name, title, office, and phone number of each individual having sequential possession of a system's hard drive, when it is removed due to compromise and the need for possible forensic examination of evidence for potential prosecution.  16 Establish an optimal, cost-effective, configuration for network boundary devices that includes procedures and a schedule for periodic testing of incoming filtering protection.  17 Ensure that cryptography is used for transmission of classified national security information, in accordance with the DOC Security Manual, Chapter 22  18 Ensure that remote systems are monitored for compliance with DOC policies (as technically possible)  19 Notify managers, supervisors, or COTRs to pursue appropriate disciplinary action and termination of remote user access privileges when users violate DOC policies.		(b) Rules of hehavior/accentable use policies:			
(c) Segregation of duties; and (d) Personnel termination and transfer.  ITSPP 3.6.3  (d) Personnel termination and transfer.  ITSPP 3.6.4, RASP  13 Ensure that all operating unit employees understand software copyright rules of behavior guidance.  14 Establish a process to identify, track, and report on security patch management.  15 Establish a Chain of Custody that documents (in writing) the name, title, office, and phone number of each individual having sequential possession of a system's hard drive, when it is removed due to compromise and the need for possible forensic examination of evidence for potential prosecution.  16 Establish an optimal, cost-effective, configuration for network boundary devices that includes procedures and a schedule for periodic testing of incoming filtering protection.  17 Ensure that cryptography is used for transmission of classified national security information, in accordance with the DOC Security Manual, Chapter 22  18 Ensure that remote systems are monitored for compliance with DOC policies (as technically possible)  19 Notify managers, supervisors, or COTRs to pursue appropriate disciplinary action and termination of remote user access privileges when users violate DOC policies.		(b) Rules of behavior/acceptable use policies,	1		
(d) Personnel termination and transfer.  ITSPP 3.6.4, RASP  13 Ensure that all operating unit employees understand software copyright rules of behavior guidance.  14 Establish a process to identify, track, and report on security patch management.  15 Establish a Chain of Custody that documents (in writing) the name, title, office, and phone number of each individual having sequential possession of a system's hard drive, when it is removed due to compromise and the need for possible forensic examination of evidence for potential prosecution.  16 Establish an optimal, cost-effective, configuration for network boundary devices that includes procedures and a schedule for periodic testing of incoming filtering protection.  17 Ensure that cryptography is used for transmission of classified national security information, in accordance with the DOC Security Manual, Chapter 22  18 Ensure that remote systems are monitored for compliance with DOC policies (as technically possible)  19 Notify managers, supervisors, or COTRs to pursue appropriate disciplinary action and termination of remote user access privileges when users violate DOC policies.		(c) Segregation of duties: and			
13 Ensure that all operating unit employees understand software copyright rules of behavior guidance.  14 Establish a process to identify, track, and report on security patch management.  15 Establish a Chain of Custody that documents (in writing) the name, title, office, and phone number of each individual having sequential possession of a system's hard drive, when it is removed due to compromise and the need for possible forensic examination of evidence for potential prosecution.  16 Establish an optimal, cost-effective, configuration for network boundary devices that includes procedures and a schedule for periodic testing of incoming filtering protection.  17 Ensure that cryptography is used for transmission of classified national security information, in accordance with the DOC Security Manual, Chapter 22  18 Ensure that remote systems are monitored for compliance with DOC policies (as technically possible)  19 Notify managers, supervisors, or COTRs to pursue appropriate disciplinary action and termination of remote user access privileges when users violate DOC policies.					
13 Ensure that all operating unit employees understand software copyright rules of behavior guidance.  14 Establish a process to identify, track, and report on security patch management.  15 Establish a Chain of Custody that documents (in writing) the name, title, office, and phone number of each individual having sequential possession of a system's hard drive, when it is removed due to compromise and the need for possible forensic examination of evidence for potential prosecution.  16 Establish an optimal, cost-effective, configuration for network boundary devices that includes procedures and a schedule for periodic testing of incoming filtering protection.  17 Ensure that cryptography is used for transmission of classified national security information, in accordance with the DOC Security Manual, Chapter 22  18 Ensure that remote systems are monitored for compliance with DOC policies (as technically possible)  19 Notify managers, supervisors, or COTRs to pursue appropriate disciplinary action and termination of remote user access privileges when users violate DOC policies.		(d) I cronner termination and transfer.			
behavior guidance.  14 Establish a process to identify, track, and report on security patch management.  15 Establish a Chain of Custody that documents (in writing) the name, title, office, and phone number of each individual having sequential possession of a system's hard drive, when it is removed due to compromise and the need for possible forensic examination of evidence for potential prosecution.  16 Establish an optimal, cost-effective, configuration for network boundary devices that includes procedures and a schedule for periodic testing of incoming filtering protection.  17 Ensure that cryptography is used for transmission of classified national security information, in accordance with the DOC Security Manual, Chapter 22  18 Ensure that remote systems are monitored for compliance with DOC policies (as technically possible)  19 Notify managers, supervisors, or COTRs to pursue appropriate disciplinary action and termination of remote user access privileges when users violate DOC policies.	12	Ensura that all operating unit amployees understand software convigant rules of			
14 Establish a process to identify, track, and report on security patch management.  15 Establish a Chain of Custody that documents (in writing) the name, title, office, and phone number of each individual having sequential possession of a system's hard drive, when it is removed due to compromise and the need for possible forensic examination of evidence for potential prosecution.  16 Establish an optimal, cost-effective, configuration for network boundary devices that includes procedures and a schedule for periodic testing of incoming filtering protection.  17 Ensure that cryptography is used for transmission of classified national security information, in accordance with the DOC Security Manual, Chapter 22  18 Ensure that remote systems are monitored for compliance with DOC policies (as technically possible)  19 Notify managers, supervisors, or COTRs to pursue appropriate disciplinary action and termination of remote user access privileges when users violate DOC policies.			11311 3.10.4.1		
15 Establish a Chain of Custody that documents (in writing) the name, title, office, and phone number of each individual having sequential possession of a system's hard drive, when it is removed due to compromise and the need for possible forensic examination of evidence for potential prosecution.  16 Establish an optimal, cost-effective, configuration for network boundary devices that includes procedures and a schedule for periodic testing of incoming filtering protection.  17 Ensure that cryptography is used for transmission of classified national security information, in accordance with the DOC Security Manual, Chapter 22  18 Ensure that remote systems are monitored for compliance with DOC policies (as technically possible)  19 Notify managers, supervisors, or COTRs to pursue appropriate disciplinary action and termination of remote user access privileges when users violate DOC policies.			ITCDD 2 10 6 1		
and phone number of each individual having sequential possession of a system's hard drive, when it is removed due to compromise and the need for possible forensic examination of evidence for potential prosecution.  16 Establish an optimal, cost-effective, configuration for network boundary devices that includes procedures and a schedule for periodic testing of incoming filtering protection.  17 Ensure that cryptography is used for transmission of classified national security information, in accordance with the DOC Security Manual, Chapter 22  18 Ensure that remote systems are monitored for compliance with DOC policies (as technically possible)  19 Notify managers, supervisors, or COTRs to pursue appropriate disciplinary action and termination of remote user access privileges when users violate DOC policies.					
hard drive, when it is removed due to compromise and the need for possible forensic examination of evidence for potential prosecution.  16 Establish an optimal, cost-effective, configuration for network boundary devices that includes procedures and a schedule for periodic testing of incoming filtering protection.  17 Ensure that cryptography is used for transmission of classified national security information, in accordance with the DOC Security Manual, Chapter 22  18 Ensure that remote systems are monitored for compliance with DOC policies (as technically possible)  19 Notify managers, supervisors, or COTRs to pursue appropriate disciplinary action and termination of remote user access privileges when users violate DOC policies.			11SPP 3.14.12		
forensic examination of evidence for potential prosecution.  16 Establish an optimal, cost-effective, configuration for network boundary devices that includes procedures and a schedule for periodic testing of incoming filtering protection.  17 Ensure that cryptography is used for transmission of classified national security information, in accordance with the DOC Security Manual, Chapter 22  18 Ensure that remote systems are monitored for compliance with DOC policies (as technically possible)  19 Notify managers, supervisors, or COTRs to pursue appropriate disciplinary action and termination of remote user access privileges when users violate DOC policies.					
16 Establish an optimal, cost-effective, configuration for network boundary devices that includes procedures and a schedule for periodic testing of incoming filtering protection.  17 Ensure that cryptography is used for transmission of classified national security information, in accordance with the DOC Security Manual, Chapter 22  18 Ensure that remote systems are monitored for compliance with DOC policies (as technically possible)  19 Notify managers, supervisors, or COTRs to pursue appropriate disciplinary action and termination of remote user access privileges when users violate DOC policies.					
that includes procedures and a schedule for periodic testing of incoming filtering protection.  17 Ensure that cryptography is used for transmission of classified national security information, in accordance with the DOC Security Manual, Chapter 22  18 Ensure that remote systems are monitored for compliance with DOC policies (as technically possible)  19 Notify managers, supervisors, or COTRs to pursue appropriate disciplinary action and termination of remote user access privileges when users violate DOC policies.			ITCDD 2 16 2 2		
protection.  17 Ensure that cryptography is used for transmission of classified national security information, in accordance with the DOC Security Manual, Chapter 22  18 Ensure that remote systems are monitored for compliance with DOC policies (as technically possible)  19 Notify managers, supervisors, or COTRs to pursue appropriate disciplinary action and termination of remote user access privileges when users violate DOC policies.					
17 Ensure that cryptography is used for transmission of classified national security information, in accordance with the DOC Security Manual, Chapter 22  18 Ensure that remote systems are monitored for compliance with DOC policies (as technically possible)  19 Notify managers, supervisors, or COTRs to pursue appropriate disciplinary action and termination of remote user access privileges when users violate DOC policies.			and 3.16.3.5		
information, in accordance with the DOC Security Manual, Chapter 22  18 Ensure that remote systems are monitored for compliance with DOC policies (as technically possible)  19 Notify managers, supervisors, or COTRs to pursue appropriate disciplinary action and termination of remote user access privileges when users violate DOC policies.		I .	TTCDD 0 1 6 7 0		
Ensure that remote systems are monitored for compliance with DOC policies (as technically possible)  19 Notify managers, supervisors, or COTRs to pursue appropriate disciplinary action and termination of remote user access privileges when users violate DOC policies.			11SPP 3.16.7.3		
technically possible)  RASP  Notify managers, supervisors, or COTRs to pursue appropriate disciplinary action and termination of remote user access privileges when users violate DOC policies.					
19 Notify managers, supervisors, or COTRs to pursue appropriate disciplinary action and termination of remote user access privileges when users violate DOC policies.		· · · · · · · · · · · · · · · · · · ·	· ·		
action and termination of remote user access privileges when users violate DOC policies.					
policies.			RASP		
*		• •			
20 Engure that the network warning benner communicates that there is no ITSDD 2.6.2.2		<u> </u>			
20 Ensure that the network warning banner communicates that there is no 115PF 5.0.2.5	20	Ensure that the network warning banner communicates that there is no	ITSPP 3.6.2.3		
expectation of privacy in the authorized or unauthorized use of DOC IT systems		expectation of privacy in the authorized or unauthorized use of DOC IT systems			

v1 02/28/2003 2